AF
Ca 2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Ca et al.
Case: 2
Serial No.: 09/876,568
Filing Date: June 7, 2001
Group: 2134
Examiner: Piotr Poltorak

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature: Dina Maurice Date: February 14, 2006

Title: Method and Apparatus for Protecting a Device Connected to a Network

---

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

1. Appeal Brief; and
2. Copy of Notice of Appeal, filed on December 15, 2005, with copy of stamped return postcard indicating receipt of Notice by PTO on December 19, 2005.

There is an additional fee of $500 due in conjunction with this submission under 37 CFR §1.17(c). Please charge **Deposit Account No. 50-0762** the amount of $500, to cover this fee. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 50-0762** as required to correct the error. A duplicate copy of this letter is enclosed.

Respectfully,

Kevin M. Mason

Date: February 14, 2006

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	Ca et al.
Case:	3-2
Serial No.:	09/876,568
Filing Date:	June 7, 2001
Group:	2134
Examiner:	Piotr Poltorak

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. 1450, Alexandria, VA 22313-1450.

Signature: Gina Mauro Date: February 14, 2006

Title: Method and Apparatus for Protecting a Device Connected to a Network

---

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby appeal the final rejection dated August 9, 2005, of claims 1 through 32 of the above-identified patent application.

REAL PARTY IN INTEREST

The present application is assigned to Agere Systems Inc., as evidenced by a Statement under 37 CFR 3.73(b) recorded on April 16, 2003. The assignee, Agere Systems Inc., is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1 through 32 are pending in the above-identified patent application. Claims 1, 10, 17, 22, 26-29, and 31-32 remain rejected under 35 U.S.C. §102(b) as being anticipated by Thurrott (Paul Thurrott, "What's New in Windows 2000 RC2 Reviewed," http://www.winsupersite.com/reviews/win2k_rc2_whatsnew.asp), claims 1, 7-10, 12, 17, 22, 26-29, and 31-32 remain rejected under 35 U.S.C. §102 as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over Cromer et al. (United States Patent Number 6,021,493), claims 2-3, 13-14, 18-19, and 23-24 remain rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sanders et al. (United States Patent Number 5,231,375) and further in view of Lam (United States Patent Number 6,140,923), claims 3, 14, 19, and 24 remain rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Minasi (Mark Minasi, "Mastering Windows NT Server 4," 6th edition, 1999, ISBN: 0782124453), claims 4 and 5 remain rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Pearce (United States Patent Number 6,308,272), and claims 6, 11, 15-16, 20-21, 25, and 30 remain rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sobell (Mark G. Sobell, "A Practical Guide to the UNIX System," 3rd edition, 1997, ISBN: 0805375651).

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to a method and apparatus for detecting the removal of a device connected to a network. The present invention generates an alarm on a protected device when an unauthorized user disconnects the device from a network connection. (Page 2, line 24, to page 4, line 7.) The network connection is monitored and an alarm is generated if the protected device is disconnected from the network connection without proper notification to the theft protection utility. (Page 4,

line 8, to page 5, line 29.) A number of fail-safe features can optionally be employed to ensure that the theft protection aspects of the present invention are not bypassed. For example, the theft protection utility process can employ speaker, volume and/or power control features to ensure that the alarms generated by the present invention, or the theft protection feature itself, cannot be bypassed. (Page 4, line 24, to page 5, line 12.) In particular, the present specification discloses monitoring a network connection (page 5, lines 13-29); and generating an alarm in a removed device if the network connection is disconnected (page 5, lines 25-29), discloses sending a message to a second device connected to a network that will initiate a response; and generating an alarm in a removed device if a response is not received within a predefined time interval (page 5, lines 13-29), and discloses monitoring a signal received on a network connection from a remote device over the network connection; and generating an alarm in a removed device if said signal is no longer received (page 5, lines 13-29).

STATEMENT OF GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 10, 17, 22, 26-29, and 31-32 are rejected under 35 U.S.C. §102(b) as being anticipated by Thurrott, claims 1, 7-10, 12, 17, 22, 26-29, and 31-32 are rejected under 35 U.S.C. §102 as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over Cromer et al., claims 2-3, 13-14, 18-19, and 23-24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sanders et al. and further in view of Lam, claims 3, 14, 19, and 24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Minasi, claims 4 and 5 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Pearce, and claims 6, 11, 15-16, 20-21, 25, and 30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sobell.

ARGUMENT

Independent Claims 1, 12, 17, 22, 31 and 32

Independent claims 1, 17, 22, and 31-32 are rejected under 35 U.S.C. §102(b) as being anticipated by Thurrott, and claims 1, 12, 17, 22, and 31-32 are rejected under 35 U.S.C. §102 as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over Cromer et al. Regarding claim 1, the Examiner asserts that Thurrott teaches monitoring a network connection and generating an alarm if the network connection is disconnected. Also, regarding claim 1, the Examiner asserts that even if disconnection of the remote computer system did not result in the generation of the alarm, it would have been obvious to one of ordinary skill in the art to implement such a modification. In the Advisory Action, the Examiner asserts that Cromer teaches that, "if the device is disconnected (removed) from the network it will not receive response to its polls and will attempt to send a message to an administrator." (See, Cromer, col. 7, lines 31-54.) The Examiner further asserts that "the computer must be alerted to the fact that a particular event occurred (no response to polling has been received)."

Appellants note that Thurrott teaches that "a new ***visual cue*** has been added to *alert* ***the user*** when the machine is disconnected from the network." (Network Disconnect Cue section.) Thurrott teaches that a *visual cue alerts the user*. If a machine is not being used, a theft alarm must alert one or more people who are ***not*** users. Thus, a visual cue that alerts a user of a machine is unlikely to be effective as an alarm to alert one or more individuals to a theft, as would be apparent to a person of ordinary skill in the art. Thus, a person of ordinary skill in the art would not interpret the visual cue disclosed by Thurrott as an alarm for indicating a theft.

Appellants also note that Cromer is directed to a method for detecting when a computer system has been disconnected from a data transmission network that "includes providing a plurality of computer systems connected to a main computer system via a data transmission network, each of said plurality of computer systems having a network connector for communicating data with the main computer." (Col. 2, lines 39-46.) An alert message is sent "from the main computer to a *network*

administrator only if it is determined that at least one of the plurality of computer systems is not connected to the network." (Col. 2, lines 52-55; emphasis added; see, also, col. 7, lines 31-54, and col. 9, lines 18-30.) Cromer, however, does not disclose or suggest generating an alarm in the *removed device*. Cromer, in fact, actually teaches away from the present invention by teaching to install an alarm outside of the protected device. Thus, a person of ordinary skill in the art would not look to modify the system disclosed by Cromer to incorporate an alarm *in the protected device*.

Regarding the Examiner's assertion that, "if the device is disconnected (removed) from the network it will not receive response to its polls and will attempt to send a message to an administrator," Appellants note that Cromer teaches that,

> *when the client receives this packet it transmits a packet back to the LAN indicating it is still on the LAN.* ***If the software application gets a response back then it just moves to the next client. If the software application does not get a response back after a predetermined number of retries, it indicates to the LAN administrator though a message*** that the client at this location is now not attached to the LAN anc can be assumed missing or stolen.
> (Col. 7, lines 41-49; emphasis added.)

Thus, contrary to the Examiner's assertion, Cromer discloses that the software application that receives the response from the client (and *not* the client) is the application that sends a message to the LAN administrator. Independent claims 1, 22, 31, and 32 require *generating an alarm in said removed device* if said network connection is disconnected. Independent claim 12 requires *generating an alarm in said removed device* if said response is not received within a predefined time interval. Independent claim 17 requires *generating an alarm in said removed device* if said signal is no longer received.

Thus, Thurrott and Cromer et al., alone or in combination, do not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, do not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and do not

disclose or suggest generating an alarm in said removed device if said signal is no longer received and a theft detection mode is enabled, as required by independent claim 17.

Additional Cited References

Sanders et al. was also cited by the Examiner for its disclosure of a device connected to a network by a network connection that produces an audible alarm signal in the device. Appellants note that Sanders teaches that,

> in accordance with the present invention, whenever data processing equipment or electronic equipment 1000 is disconnected from DCM 1020, ***theft detection and alarm system 1010 generates an alarm data signal*** which is transmitted to DCM 1020 and, optionally, ***theft detection and alarm system 1010 generates an alarm at its physical location***. In response to the data signal from theft detection and alarm system 1010, DCM 1020 transmits an alarm status code to CBX 1030. In response, the above-described applications program in CBX 1030 transmits the alarm status code to theft and alarm system monitor 1050 along with configuration information related to DCM 1020. Once again, theft and alarm system monitor 1050 utilizes the status information, including the DCM configuration information, as a retrieval key to access database 1060 and to retrieve information which relates to the disconnected equipment. Then, theft and alarm system monitor generates a report which identifies the particular equipment which was disconnected. The report may be printed at a terminal in a central location and/or may be printed at security location in the vicinity of the disconnected DCM and/or may be printed at a security dispatch location and so forth.
>
> In either case, whether DCM 1020 or data processing or electronic equipment 1000 is disconnected, theft detection and alarm system monitor 1050 can send a message, in a manner which is well known to those of ordinary skill in the art, to a security terminal and/or cause ***an alarm to be sounded in the area of the disconnected equipment*** and/or place a telephone call to a predetermined security location and/or transmit a predetermined message to an external loud speaker, using CBX 1030. Further, various such strategies could be implemented as various times during the day. For example, alarm generations in response to disconnect information may be disabled at theft alarm system monitor 1050 during the day and activated during the night or on the week-end when most thefts are expected to occur. Further, alarm generation in response to disconnect information may be disabled at theft alarm system monitor 1050 on an equipment or location basis to enable one to move equipment.
>
> (Col. 4, lines 26-68; emphasis added.)

Sanders, however, does ***not*** disclose or suggest generating an alarm in the *removed device*.

Thus, Sanders et al. do not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, do not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and do not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

Lam was also cited by the Examiner for its disclosure of motivation to combine Sanders and Cromer. Lam, however, does ***not*** address the issue of devices connected to a network.

Thus, Lam does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

Minasi was also cited by the Examiner for its disclosure of assigning rights to users that grant or deny access to certain objects (resources) such as turning off a device. Appellants note that Minasi is directed to registry control in an operating system, user rights, and object permissions. Minasi does ***not*** address the issue of detecting the removal of a device connected to a network.

Thus, Minasi does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent

claim 17.

Pearce was also cited by the Examiner for its disclosure of monitoring that is set to activate automatically in a passive manner. Appellants note that Pearce is directed to a "security system using a security detector associated with a personal computer attached to an existing data transmission network, where the personal computer is effective to detect security breaches and transmit an alarm." (See, Abstract.) Pearce does ***not*** address the issue of detecting the removal of a device connected to a network.

Thus, Pearce does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

Sobell was also cited by the Examiner for its disclosure of using a password to perform administrative tasks. Appellants note that Sobell is a guide to a UNIX system. Sobell does ***not*** address the issue of detecting the removal of a device connected to a network.

Thus, Sobell does not disclose or suggest generating an alarm in said removed device if said network connection is disconnected, as required by independent claims 1, 22, 31, and 32, does not disclose or suggest generating an alarm in said removed device if said response is not received within a predefined time interval, as required by independent claim 12, and does not disclose or suggest generating an alarm in said removed device if said signal is no longer received, as required by independent claim 17.

<u>Claims 2, 13, 18 and 23</u>

Claims 2, 13, 18, and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sanders et al. and further in view of Lam. In particular, the Examiner acknowledges that Cromer et al. do not teach preventing a

volume of an audio output of the device from being reduced below a predefined minimum level, but asserts that Sanders teaches this limitation (FIG. 2; col. 5, lines 33-38).

In the text cited by the Examiner, Sanders teaches that the "theft detection and alarm system 1010 produces an audible alarm signal whenever there is a sustained absence of signal current in either of cables 14 and 15 and it sends an alarm data signal to electronic unit 1020 if, for example, electronic unit 1020 is embodied as a DCM and there is an absence of current in cable 14." (Col. 5, lines 33-38.) Contrary to the Examiner's assertion, Sanders does ***not*** disclose or suggest preventing a volume of an audio output of the device from ***being reduced below a predefined minimum level.***

Thus, Thurrott, Cromer et al., Sanders et al., Lam, Minasi, Pearce et al., and Sobell, alone or in any combination, do not disclose or suggest preventing a volume of an audio output of the device from being reduced below a predefined minimum level, as required by claims 2, 13, 18, and 23.

Claims 3, 14, 19 and 24

Claims 3, 14, 19, and 24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Sanders et al. and further in view of Lam, and claims 3, 14, 19, and 24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al. in view of Minasi. In particular, the Examiner asserts that Sanders teaches preventing the device from being turned off (FIG. 6 and col. 11, lines 46-49), and that Minasi teaches assigning rights to users that grant or deny access to certain objects (resources) such as turning off a device (page 378, section 3, and "shut down rights" on page 380).

In the text cited by the Examiner, Sanders teaches that the "theft detection and alarm system 1010 comprises power supply circuitry (not shown) which generates the voltages needed for the operation thereof." (Col. 11, lines 46-49.) Contrary to the Examiner's assertion, Sanders does ***not*** disclose or suggest *preventing said device from being turned off.* In addition, Appellants could find no disclosure or suggestion in either Cromer or Minasi to combine the invention disclosed by Cromer and the user rights

methods disclosed by Minasi.

Thus, Thurrott, Cromer et al., Sanders et al., Lam, Minasi, Pearce, and Sobell, alone or in any combination, do not disclose or suggest preventing said device from being turned off, as required by claims 3, 14, 19, and 24.

Conclusion

The rejections of the cited claims under sections 102 and 103 in view of Thurrott, Cromer et al., Sanders et al., Lam, Minasi, Pearce, and Sobell, alone or in any combination, are therefore believed to be improper and should be withdrawn. The remaining rejected dependent claims are believed allowable for at least the reasons identified above with respect to the independent claims.

The attention of the Examiner and the Appeal Board to this matter is appreciated.

Respectfully,

Date: February 14, 2006

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560

APPENDIX

1. A method for detecting removal of a device connected to a network by a network connection, comprising:

monitoring said network connection; and

generating an alarm in said removed device if said network connection is disconnected.

2. The method of claim 1, further comprising the step of preventing a volume of an audio output of said device from being reduced below a predefined minimum level.

3. The method of claim 1, further comprising the step of preventing said device from being turned off.

4. The method of claim 1, wherein said monitoring step is automatically activated in a passive manner.

5. The method of claim 1, wherein said monitoring step is manually activated by a user.

6. The method of claim 1, wherein said generating step can be prevented by entering a password.

7. The method of claim 1, wherein said monitoring step further comprises the step of sending a message to a remote device and awaiting a response.

8. The method of claim 1, wherein said monitoring step further comprises the step of receiving a message from a remote device.

9. The method of claim 1, wherein said monitoring step further comprises the step of receiving a signal from a remote device.

10. The method of claim 1, wherein said monitoring step further comprises the step of polling one or more local network ports on said device.

11. The method of claim 1, wherein said generating step is performed only if said network connection is disconnected by an unauthorized user.

12. A method for detecting removal of a device connected to a network by a network connection, comprising:

sending a message to a second device connected to said network that will initiate a response; and

generating an alarm in said removed device if said response is not received within a predefined time interval.

13. The method of claim 12, further comprising the step of preventing a volume of an audio output of said device from being reduced below a predefined minimum level.

14. The method of claim 12, further comprising the step of preventing said device from being turned off.

15. The method of claim 12, wherein said generating step can be prevented by entering a password.

16. The method of claim 12, wherein said generating step is performed only if said network connection is disconnected by an unauthorized user.

17. A method for detecting removal of a device connected to a network by a network connection, comprising:

monitoring a signal received on said network connection from a remote device over said network connection; and

generating an alarm in said removed device if said signal is no longer received.

18. The method of claim 17, further comprising the step of preventing a volume of an audio output of said device from being reduced below a predefined minimum level.

19. The method of claim 17, further comprising the step of preventing said device from being turned off.

20. The method of claim 17, wherein said generating step can be prevented by entering a password.

21. The method of claim 17, wherein said generating step is performed only if said network connection is disconnected by an unauthorized user.

22. A system for detecting removal of a device connected to a network by a network connection, comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

monitor said network connection; and

generate an alarm in said removed device if said network connection is disconnected.

23. The system of claim 22, wherein said processor is further configured to prevent a volume of an audio output of said device from being reduced below a predefined minimum level.

24. The system of claim 22, wherein said processor is further configured to prevent said device from being turned off.

25. The system of claim 22, wherein said processor is further configured to prevent said alarm by entering a password.

26. The system of claim 22, wherein said processor is further configured to send a message to a remote device and await a response.

27. The system of claim 22, wherein said processor is further configured to receive a message from a remote device.

28. The system of claim 22, wherein said processor is further configured to receive a signal from a remote device.

29. The system of claim 22, wherein said processor is further configured to poll one or more local network ports on said device.

30. The system of claim 22, wherein said processor is further configured to generate said alarm only if said network connection is disconnected by an unauthorized user.

31. An article of manufacture for detecting removal of a device connected to a network by a network connection, comprising:

a computer readable medium having computer readable code means

embodied thereon, said computer readable program code which when executed implements the steps of:

a step to monitor said network connection; and

a step to generate an alarm in said removed device if said network connection is disconnected.

32. A system for detecting removal of a device connected to a network by a network connection, comprising:

means for monitoring said network connection; and

means for generating an alarm in said removed device if said network connection is disconnected.

EVIDENCE APPENDIX

There is no evidence submitted pursuant to § 1.130, 1.131, or 1.132 or entered by the Examiner and relied upon by appellant.

RELATED PROCEEDINGS APPENDIX

There are no known decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 CFR 41.37.

PTO/SB/31 (02-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Docket Number (Optional): Ca 3-2

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Assistant Commissioner for Patents, Washington D.C. 20231" on December 15, 2005.

Signature: Tina Maurice

Typed or printed name: Tina Maurice

In re Application of: Ca et al.

Application Number	Filed
09/876,568	June 7, 2001

For: Method and Apparatus for Protecting a Device Connected to a Network

Group Art Unit	Examiner
2134	Piotr Poltorak

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 1.17(b)) $500.00.

- ☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $_____.
- ☐ A check in the amount of the fee is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Commissioner has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of this sheet.
- ☑ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0762. I have enclosed a duplicate copy of this sheet.
- ☑ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record.
- ☐ attorney or agent acting under 37 CFR 1.34(a). Registration number if acting under 37 CFR 1.34(a)._____.

Kevin M. Mason
Signature

Kevin M. Mason
Typed or printed name

December 15, 2005
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

Ryan, Mason & Lewis, LLP
Attorneys At Law
1300 Post Road
Suite 205
Fairfield, Ct 06824

Receipt in the USPTO is hereby acknowledged of:

Transmittal Letter – (Original & 1 copy)
Notice of Appeal - (Original & 1 copy)
Petition for Extension of Time – (Original & 1 copy)

Case Name: Ca 3-2
Serial No.: 09/876,568

1150-1005

December 15, 2005 KMM